

GALOIS EXTENSIONS OF HEIGHT-ONE COMMUTING DYNAMICAL SYSTEMS

GHASSAN SARKIS AND JOEL SPECTER

ABSTRACT. We consider a dynamical system consisting of a pair of commuting power series, one noninvertible and another nontorsion invertible, of height one with coefficients in the p -adic integers. Assuming that each point of the dynamical system generates a Galois extension over the base field, we show that these extensions are in fact abelian, and, using results and considerations from the theory of the field of norms, we also show that the dynamical system must include a torsion series of maximal order. From an earlier result, this shows that the series must in fact be endomorphisms of some height-one formal group.

1. INTRODUCTION

The study of p -adic dynamical systems has seen increased interest over the past two decades, reflected most recently in a new MSC category: *Arithmetic and non-Archimedean dynamical systems*. This note is concerned with three overlapping ways of looking at such systems—formal power series that commute under composition, iterated morphisms of the open p -adic unit disc, and galoisness of extensions that are obtained by adjoining zeros of dynamical systems. Indeed, the proof of the main result in this note can be viewed as relating commuting power series to formal groups, analytic maps of the open unit disk to locally analytic galois automorphisms, and galois towers to automorphism subgroups of residue fields.

1.1. Notation and motivation. Our power series have no constant term in order for composition to be well defined and finitary. Also, their linear coefficients are nonzero to exclude trivial cases. We adopt therefore some of the notation of [8]. Let $g^{(n)}$ be the n -fold iterate of g with itself under composition. For a commutative ring R , let $\mathcal{S}_0(R) = \{g \in R[[x]] \mid g(0) = 0 \text{ and } g'(0) \neq 0\}$. Let $\mathcal{G}_0(R) = \{g \in \mathcal{S}_0(R) \mid g'(0) \in R^\times\}$ be the group of series that are invertible under composition.

Suppose F is a finite extension of \mathbb{Q}_p with ring of integers \mathcal{O} , maximal ideal \mathfrak{m} , and residue field $\kappa = \mathcal{O}/\mathfrak{m}$. Denote by v_F the unique additive valuation on any algebraic extension of F normalized so that $v_F(F^\times) = \mathbb{Z}$; for simplicity, v_p will be used instead of $v_{\mathbb{Q}_p}$. Let $\mathfrak{m}^{\text{alg}}$ be the maximal ideal in the integral closure of \mathcal{O} in F^{alg} , an algebraic closure of F .

The *Newton Polygon* of $g(x) = \sum a_i x^i \in \mathcal{O}[[x]]$, denoted $\mathcal{N}(g)$, is the convex hull of the sequence of points $(i, v_F(a_i))$. If $\mathcal{N}(g)$ has a segment of horizontal length ℓ and slope λ , then g has, counting multiplicity, precisely ℓ roots in F^{alg} of F -valuation λ . We are interested in roots that lie in $\mathfrak{m}^{\text{alg}}$; these correspond to

2010 *Mathematics Subject Classification.* 11S31, 37P20 (primary), 14L05, 11S15 (secondary).
The authors were partially supported by NSF Grant DMS-0755540.

segments of the Newton polygon of negative slope. To that end, we define $\mathcal{N}^-(g)$ to be the portion of $\mathcal{N}(g)$ consisting of segments whose slopes are negative.

Let $\bar{g}(x) = \sum \bar{a}_i x^i \in \kappa[[x]]$ be the coefficientwise reduction of g to κ . The *Weierstrass degree* of \bar{g} , denoted $\text{ord}_x(\bar{g})$, is defined to equal ∞ if $\bar{g} = 0$, and $\min\{i \mid \bar{a}_i \neq 0\}$ otherwise; the Weierstrass degree of g is defined to equal $\text{ord}_x(\bar{g})$. The *p-adic Weierstrass Preparation Theorem* (WPT) asserts that if $\text{ord}_x(g) < \infty$ then there exists a unique factorization $g(x) = P(x)U(x)$, where $P(x) \in \mathcal{O}[x]$ is monic of degree $\text{ord}_x(g)$ and $U(x) \in \mathcal{O}[[x]]$ has a multiplicative inverse, and hence no zeroes in $\mathfrak{m}^{\text{alg}}$. Moreover, the roots of $P(x)$ and $g(x)$ in $\mathfrak{m}^{\text{alg}}$ coincide; consequently, so do $\mathcal{N}(P)$ and $\mathcal{N}^-(g)$. See [5, Chapter IV] for a more details on Newton polygons.

If $f, u \in \mathcal{S}_0(\mathcal{O})$ such that f is noninvertible and u is invertible, let

$$\begin{aligned} \Lambda_f(n) &= \{\pi \in \mathfrak{m}^{\text{alg}} \mid f^{\circ n}(\pi) = 0\} & \text{and} & \quad \Lambda_f = \bigcup_{n \geq 0} \Lambda_f(n); \\ \Lambda_u(n) &= \{\pi \in \mathfrak{m}^{\text{alg}} \mid u^{\circ p^n}(\pi) = \pi\} & \text{and} & \quad \Lambda_u = \bigcup_{n \geq 0} \Lambda_u(n). \end{aligned}$$

Observe that $n \geq 0$, $\Lambda_f(n+1) \setminus \Lambda_f(n)$ consists of roots of $f(x) - \pi$ as π ranges through $\Lambda_f(n) \setminus \Lambda_f(n-1)$. Let $\Omega_f(n) = \Lambda_f(n) \setminus \Lambda_f(n-1)$.

Although formal groups are not explicitly visible in our results, they provide part of the motivation, which we discuss briefly next. We will call $f, u \in \mathcal{S}_0(\mathcal{O})$ a *commuting pair* if f is noninvertible and u is nontorsion invertible. Commuting pairs share certain characteristic properties with formal group endomorphisms. For example, $\Lambda_f = \Lambda_u$ by [8, Proposition 3.2]. Also, $\text{ord}_x(f)$ is either infinite or a power of p by [8, Main Theorem 6.3]. Both of these results are important properties of formal group endomorphisms. Thus, Lubin suggested that commutativity may be enough to indicate the existence of “a formal group somehow in the background” [8, page 341]. Counterexamples to naïve statements and proofs of special cases of this conjecture are both known, though a general case remains elusive. For a more detailed discussion of the issues involved in a precise statement of the conjecture, see [11].

Let $e = p - 1$ if $p > 2$ and $e = 2$ if $p = 2$. The following special case of Lubin’s conjecture, proven in [11, Theorem 1.1], makes use of a torsion third series of order e in the dynamical system:

Theorem 1.1. *Let $f, u, z \in \mathcal{S}_0(\mathbb{Z}_p)$ such that f, u is a commuting pair with $\text{ord}_x(f) = p$ and $v_p(f'(0)) = v_p(u'(0) - 1) = 1$, and if $p = 2$ then additionally $v_2(u'(0)^2 - 1) = 3$. Suppose also that z is torsion of order e and commutes with f . Then there exists a formal group F over \mathbb{Z}_p such that $f, u, z \in \text{End}_{\mathbb{Z}_p}(F)$.*

It is a straightforward corollary to this theorem that $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$. We will show that, conversely, the Galoisness of $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is sufficient to guarantee the existence of the torsion series.

Let $\delta = 1$ if $p > 2$ and $\delta = 2$ if $p = 2$. We will call a commuting pair $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ *minimal* when

- $\text{ord}_x(f) = p$;
- $v_p(f'(0)) = 1$; and
- $v_p(u'(0) - 1) = \delta$.

Note that the condition on $v_p(u'(0) - 1)$ when $p = 2$ is slightly different than the one in [11], though the two are equivalent in the contexts we consider. Our main result is the following:

Main Theorem 1.2. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. If $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for each $\pi \in \Lambda_f$, then there exists a torsion series $z \in \mathcal{S}_0(\mathbb{Z}_p)$ of order e commuting with f and u .*

Remark 1.3. By [8, Propositions 1.1 and 1.2], there exists a unique power series $L_f(x) \in \mathbb{Q}_p[[x]]$ for which $L'_f(0) = 1$ and $L_f \circ f = f'(0)L_f$. And for each $a \in \mathbb{Q}_p$ there exists a unique $[a]_f \in \mathbb{Q}_p[[x]]$ such that $[a]'_f(0) = a$ and $[a]_f \circ f = f \circ [a]_f$. Let ζ_e be a primitive e^{th} root of unity, and let $z = [\zeta_e]_f \in \mathbb{Q}_p[[x]]$. In order to prove our main result, we need show only that $z \in \mathbb{Z}_p[[x]]$.

2. ROOTS AND FIXED POINTS

The integrality of the torsion series z will rely on the existence of a torsion series of the same order in $\mathcal{G}_0(\mathbb{F}_p)$ that commutes with \bar{f} and \bar{u} . More generally, it will rely on information about the structure of the normalizer of \bar{u} in $\mathcal{G}_0(\mathbb{F}_p)$ that follows from the theory of the fields of norms. We begin this section with a brief overview of fields of norms, culminating in [6, Théorème 5.9].

Suppose K is a local field with residue field κ of characteristic $p > 0$, L/K is an infinite totally ramified abelian extension, and $\mathcal{E}_{L/K} = \{E \mid K \subseteq E \subset L \text{ and } [E : K] < \infty\}$. Let $X_K(L)^* = \varprojlim_{E \in \mathcal{E}_{L/K}} E^*$, where the transition morphisms are the norm

maps, and let $X_K(L) = X_K(L)^* \cup \{0\}$. An element α of $X_K(L)$ is therefore an indexed family $(\alpha_E)_{E \in \mathcal{E}_{L/K}}$ such that whenever $E' \supseteq E$ then $N_{E'/E}(\alpha_{E'}) = \alpha_E$. Remarkably, the set of norms $X_K(L)$ turns out to be isomorphic to the local field $\kappa((x))$. Multiplication is defined in an obvious way in light of the multiplicativity of the norm map: if $\alpha, \beta \in X_K(L)$ then $\alpha\beta = (\alpha_E\beta_E)_{E \in \mathcal{E}_{L/K}}$. Addition is not as obvious: for $E \in \mathcal{E}_{L/K}$, the norms $N_{E'/E}(\alpha_{E'} + \beta_{E'})$ converge over $E' \in \mathcal{E}_{L/E}$ to an element $\gamma_E \in E$, using which one can define $\alpha + \beta = (\gamma_E)_{E \in \mathcal{E}_{L/K}}$. Finally, $v_{X_K(L)}(\alpha)$ can be defined as $v_E(\alpha_E)$, which is independent of E . The image of $\text{Gal}(L/K)$ under $X_K(*)$ is a closed subgroup of the automorphism group of $\kappa((x))$.

Conversely, certain subgroups of the automorphism group of $\kappa((x))$ arise as images of Galois groups under the field-of-norms functor. The *Nottingham group* $\text{Nott}(\kappa) = \{g(x) \in \mathcal{S}_0(\kappa) \mid g'(0) = 1\}$ has elicited interest among group theorists because every countably-based pro- p groups can be embedded in it, and as such, it contains elements of order p^n for all n ; the shape of such torsion elements will be important for the proof of our main result when $p = 2$. The Nottingham group is also the group of normalized automorphisms of the field $\kappa((x))$. Some of its subgroups, like the one generated by \bar{u} , arise as images of Galois groups under the field-of-norms functor. See [1, 4] for more information about the Nottingham group, [2, 3] for the original construction of the field of norms, and [6] for applications of the field of norms to p -adic dynamical systems that we make use of next.

If $\omega \in \text{Nott}(\kappa)$, let $i_n(\omega) = \text{ord}_x(\omega^{\circ p^n}(x) - x) - 1$. This sequence of integers, called the *lower ramification numbers* of ω , measures the rapidity with which $\omega^{\circ p^n}$ approaches the identity. According to Sen's Theorem [12], if $\omega^{\circ p^n}(x) \neq x$ then $i_n(\omega) \equiv i_{n-1}(\omega) \pmod{p^n}$. Let $e(\omega) = \lim_{n \rightarrow \infty} (p-1)i_n/p^{n+1}$. In light of Sen's Theorem, $e(\omega)$ is finite in those cases when $\omega^{\circ p^n}$ approaches the identity as slowly as possible. Note that the factor $p-1$ normalizes $e(\omega)$ so that, when finite, it is an integer.

Let $\mathcal{A}_\omega = \{\omega^{\circ a} \mid a \in \mathbb{Z}_p\}$ be the closed subgroup of \mathcal{S}_0 generated by ω . The *separable normalizer* of \mathcal{A}_ω is given by $\text{Norm}_\kappa^{\text{sep}}(\mathcal{A}_\omega) = \{\vartheta \in \kappa[[x]] \mid \vartheta' \neq 0 \text{ and } \vartheta \circ$

$\omega \circ \vartheta^{\circ-1} \in \mathcal{A}\}$. By [6, Proposition 5.5], $\text{Norm}_\kappa^{\text{sep}}(\mathcal{A}_\omega)$ is in fact a group, and [6, Théorème 5.9], quoted next, characterizes this group in the case that ω approaches the identity slowly.

Theorem 2.1. *Let κ be a perfect field and $\omega \in \mathcal{S}_0(\kappa)$ such that $e(\omega) < \infty$. Then $\text{Norm}_\kappa^{\text{sep}}(\mathcal{A}_\omega)$ is an extension of a finite group of order dividing $e(\omega)$ by the group \mathcal{A}_ω .*

Proof Outline. The field-of-norms functor associates to \mathcal{A}_ω the group $\text{Gal}(L/K)$, where L/K is an infinite abelian totally ramified extension of local fields with residue field κ . As such, the lower ramification numbers of \bar{u} correspond to the lower ramification numbers of $\text{Gal}(L/K)$, and $e(\omega)$ corresponds to the absolute ramification index of K , namely, $[K : K_0]$, where K_0 is the field of fractions of the Witt ring over κ . Let $\text{Aut}(L/K)$ be the group of automorphisms of L that send K to itself and that act trivially on the residue field. The restriction map $\text{Aut}(L/K) \rightarrow \text{Aut}(K)$ has kernel $\text{Gal}(L/K)$. The order of its image divides $[K : K_0]$. \square

2.1. The lower ramification numbers of \bar{u} . For the remainder of this section, we will consider the roots of f and its iterates in order to show that $e(\bar{u}) = e = \begin{cases} p-1 & \text{if } p > 2 \\ 2 & \text{if } p = 2 \end{cases}$, and hence apply Theorem 2.1 to $\mathcal{A}_{\bar{u}}$.

Continue to denote by F a finite extension of \mathbb{Q}_p with ring of integers \mathcal{O} , maximal ideal \mathfrak{m} , and residue field κ .

Lemma 2.2. *Suppose $f \in \mathcal{S}_0(\mathcal{O})$ such that $\text{ord}_x(f) = p$ and $v_F(f'(0)) = 1$. Then the roots of $f^{\circ n}$ in $\mathfrak{m}^{\text{alg}}$ are simple for all n . Moreover, if $\pi \in \Omega_f(n)$ then $F(\pi)/F$ is a totally ramified extension of degree $(p-1)p^{n-1}$, and π is a uniformizer in $F(\pi)$.*

Proof. Using WPT, write $f(x) = P_0(x)U_0(x)$. Note that $\Omega_f(1)$ consists of the roots of $P_0(x)/x$. By the hypothesis on f , $\mathcal{N}(P_0(x)/x)$ consists of a single segment from $(0, 1)$ to $(p-1, 0)$. So $P_0(x)/x$ is a degree $p-1$ Eisenstein polynomial over \mathcal{O} . Therefore, the roots of $P_0(x)/x$ are simple, each with F -valuation $1/(p-1)$, and each generating a degree $p-1$ totally ramified extension of F .

Proceeding by induction, assume that the result holds for some $n \geq 0$. Let $\pi \in \Omega_f(n)$. Using WPT again, write $f(x) - \pi = P_n(x)U_n(x)$, where $P_n(x) \in (\mathcal{O}[\pi])[x]$ is a polynomial whose Newton polygon consists of a single segment from $(0, 1)$ to $(p, 0)$; that is, $P_n(x)$ is a degree p Eisenstein polynomial over $\mathcal{O}[\pi]$. Thus, the roots of $f(x) - \pi$ are simple, each of $F(\pi)$ -valuation $1/p$, and each generating a degree p totally ramified extension of $F(\pi)$. Finally, if $\pi' \in \Omega_f(n)$ with $\pi' \neq \pi$, then the roots of $f(x) - \pi$ and $f(x) - \pi'$ are distinct. \square

Lemma 2.3. *Suppose $f \in \mathcal{S}_0(\mathcal{O})$ such that $\text{ord}_x(f) = p$ and $v_F(f'(0)) = 1$. Let $\pi \in \Omega_f(1)$. Then $F(\pi)/F$ is Galois. Also, for a fixed primitive $p-1$ root of unity ζ_{p-1} , and for each $0 \leq i \leq p-2$, there exists a unique $\pi^{(i)} \in \Omega_f(1)$ such that $\pi^{(i)} \equiv \zeta_{p-1}^i \pi \pmod{\mathfrak{m}^2}$.*

Proof. Using WPT as in Lemma 2.2, write $f = P_0U_0$ and note that $v_p(P_0'(0)) = 1$ and $P_0(x) \equiv x^p \pmod{p}$. Therefore, P_0 is an endomorphism of a height-one formal \mathbb{Z}_p -module (see [10]). Since the roots of f and P_0 coincide, the result follows. \square

Corollary 2.4. *$\text{Gal}(F(\pi)/F)$ is cyclic of order $p-1$.*

Proof. The Galois group is generated by $\pi \mapsto \pi^{(1)}$. \square

We next quote [11, Lemma 1.2] for reference.

Lemma 2.5. *Suppose $g_1, g_2 \in \mathcal{S}_0(\mathcal{O})$ such that $0 < v_F(g'_1(0)) = v_F(g'_2(0)) < \infty$, and every root of g_1 in $\mathfrak{m}^{\text{alg}}$ is also a root of g_2 of at least the same multiplicity. Suppose further that $g_1 \notin \mathcal{S}_0(\mathfrak{m})$. Then $\mathcal{N}^-(g_1) = \mathcal{N}^-(g_2)$, and so the roots of g_1 and g_2 in $\mathfrak{m}^{\text{alg}}$ coincide.*

Lemma 2.6. *Suppose $f, u \in \mathcal{S}_0(\mathcal{O})$ is a commuting pair such that $v_p(f'(0)) = v_p(u'(0) - 1) = 1$ and $\text{ord}_x(f) = p$. Then $\Lambda_f(1) = \Lambda_u(0)$.*

Proof. If π is a nonzero root of f , then $u(f(\pi)) = f(u(\pi)) = 0$. Thus $u(\pi)$ is another nonzero root of f , and by the hypothesis on $u'(0)$, it is in fact of the form $u(\pi) = \pi + \pi^2 d$ for some $d \in \mathbb{Z}_p[[\pi]]$. By Lemma 2.3, $u(\pi) = \pi^{(0)} = \pi$. So every root of f is also a root of $u(x) - x$. The desired conclusion follows by Lemma 2.5. \square

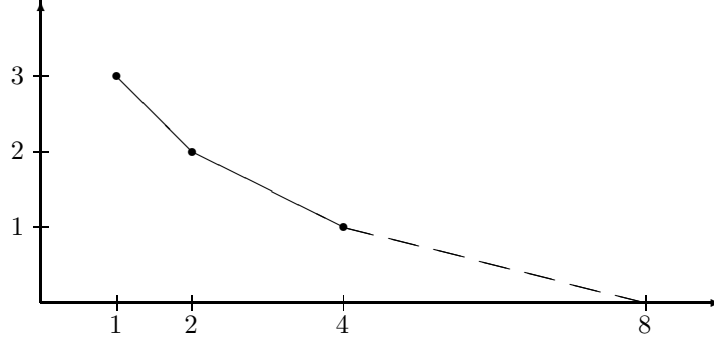
Proposition 2.7. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. Let $\delta = 1$ if $p > 2$ and $\delta = 2$ if $p = 2$. For all $n \geq \delta$, if $\pi \in \Omega_f(n+1)$, then $u^{\circ i}(\pi) = u^{\circ j}(\pi)$ if and only if $p^{n-\delta+1} \mid j - i$. Moreover, $\Lambda_f(n) = \Lambda_u(n - \delta)$.*

Proof. Suppose $p > 2$. By Lemma 2.6, $\Lambda_f(1) = \Lambda_u(0)$. Proceeding by induction, assume that $\Lambda_f(n) = \Lambda_u(n-1)$ for some $n \geq 1$. Let $\pi \in \Omega_f(n+1)$, and consider the series $f^{\circ n}(x) - f^{\circ n}(\pi)$, which has p^n roots in $\mathfrak{m}^{\text{alg}}$. Since $f^{\circ n}(\pi) \in \Lambda_f(1)$, for any $i \geq 0$ we have $u^{\circ i}(f^{\circ n}(\pi)) = f^{\circ n}(\pi) = f^{\circ n}(u^{\circ i}(\pi))$, so $u^{\circ i}(\pi) \in \Omega_f(n+1)$. Suppose that for some i and j we have $u^{\circ i}(\pi) = u^{\circ j}(\pi)$, and so $u^{\circ(j-i)}(\pi) = \pi$. If $i \neq j$, write $j - i = rp^s$ with $p \nmid r$. Applying Lemma 2.5 to $u^{\circ p^s}(x) - x$ and $u^{\circ rp^s}(x) - x$, we get $u^{\circ p^s}(\pi) = \pi$. This is impossible if $s \leq n-1$, since $\pi \notin \Lambda_f(n) = \Lambda_u(n-1) \supseteq \Lambda_u(s)$. A similar argument shows that $u^{\circ p^n}(\pi) = \pi$. Therefore, $\Lambda_f(n+1) \subseteq \Lambda_u(n)$. By Lemma 2.5, $\Lambda_f(n+1) = \Lambda_u(n)$, concluding the proof for odd primes.

Suppose $p = 2$. The inductive step of this proof will be similar to the $p > 2$ case, but we must first show that $\Lambda_f(2) = \Lambda_u(0)$ and $\Lambda_f(3) = \Lambda_u(1)$. Suppose α is the nonzero root of f . Lemma 2.2 implies $v_2(\alpha) = 1 = v_2(u(\alpha))$. Since $f(u(\alpha)) = 0$, then $\alpha \in \Lambda_u(0)$. Let β, β' be the two roots of $f(x) - \alpha$. Then $v_2(\beta) = v_2(\beta') = 1/2$. Also, $\{u(\beta), u(\beta')\} = \{\beta, \beta'\}$, so that $\beta, \beta' \in \Lambda_u(1)$. (We will later show that u fixes β and β' .) Next, let γ_1, γ_2 be the two roots of $f(x) - \beta$. Thus $u^{\circ 2}(\beta) = \beta = u^{\circ 2}(f(\gamma_1)) = f(u^{\circ 2}(\gamma_1))$, and so $u^{\circ 2}(\gamma_1) = \gamma_1$ or γ_2 . We show the impossibility of the latter case by considering $v_2(\gamma_2 - \gamma_1)$.

Recall that by Lemma 2.6, α is the only element of $\Lambda_f = \Lambda_u$ of \mathbb{Q}_2 -valuation 1, β_1 and β_2 are the only elements of \mathbb{Q}_2 -valuation $1/2$, and all other roots have \mathbb{Q}_2 -valuation $1/2^k$ for $k \geq 2$. Therefore, $\mathcal{N}^-(u^{\circ 2}(x) - x)$ must have a segment of length 1 and slope -1 , and one segment of length 2 and slope -2 , and all other segments of slope $-1/2^k$ for $k \geq 2$. The dotted line in Figure 1 corresponds to the smallest possible slope for the third segment of $\mathcal{N}^-(u^{\circ 2}(x) - x)$. So if $u^{\circ 2}(x) - x = \sum_i b_i x^i$, then $v_2(b_1) = 3$, $v_2(b_2) = 2$, $v_2(b_3) \geq 2$, $v_2(b_4) = 1$, and $v_2(b_i) \geq 1$ for $5 \leq i \leq 7$. Thus $v_2(u^{\circ 2}(\gamma_1) - \gamma_1) \geq \min_i \{v_2(b_i \gamma_1^i)\} = \min_i \{v_2(b_i) + i/4\} \geq 2$.

But γ_1 and γ_2 are roots of an Eisenstein monic quadratic polynomial over $\mathbb{Z}_p[\beta]$, and so $(\gamma_2 - \gamma_1)^2 = b^2 - 4c$, where $v_2(b) \geq v_2(c) = 1/2$. Since $v_2(b^2)$ is an integer

FIGURE 1. $\mathcal{N}^-(u^{\circ 2}(x) - x)$

while $v_2(4c) = 5/2$, the isosceles triangle principle guarantees that

$$v_2(\gamma_2 - \gamma_1) = \begin{cases} 1/2 & \text{if } v_2(b) = 1/2 \\ 1 & \text{if } v_2(b) = 1 \\ 5/4 & \text{if } v_2(b) \geq 3/2 \end{cases}$$

Therefore, $u^{\circ 2}(\gamma_1)$ cannot equal γ_2 . A similar proof shows that the roots of $f(x) - \beta'$ are fixed points of $u^{\circ 2}(x)$, so that $\Lambda_f(3) \subseteq \Lambda_u(1)$. Lemma 2.5 implies $\Lambda_f(3) = \Lambda_u(1)$. Finally, noting that $\Lambda_u(0) \subset \Lambda_u(1)$ and that u must fix two points in addition to 0 and α , we conclude that $\beta, \beta' \in \Lambda_u(0)$.

The inductive step for $p = 2$ follows a proof similar to that of $p > 2$. Assume that $\Lambda_f(n) = \Lambda_u(n - 2)$ for some $n \geq 3$. Let $\pi \in \Omega_f(n + 1)$, and consider the series $f^{\circ n}(x) - f^{\circ n}(\pi)$. Since $f^{\circ n}(\pi) \in \Lambda_f(1)$, for any $i \geq 0$ we have $u^{\circ i}(f^{\circ n}(\pi)) = f^{\circ n}(\pi) = f^{\circ n}(u^{\circ i}(\pi))$, so $u^{\circ i}(\pi) \in \Omega_f(n + 1)$. Suppose that for some i and j we have $u^{\circ i}(\pi) = u^{\circ j}(\pi)$, and so $u^{\circ(j-i)}(\pi) = \pi$. If $i \neq j$, write $j - i = r2^s$ with $2 \nmid r$. Applying Lemma 2.5 to $u^{\circ 2^s}(x) - x$ and $u^{\circ r2^s}(x) - x$, we get $u^{\circ 2^s}(\pi) = \pi$. This is impossible if $s \leq n - 2$, since $\pi \notin \Lambda_f(n) = \Lambda_u(n - 2) \supseteq \Lambda_u(s)$. A similar argument shows that $u^{\circ 2^{n-1}}(\pi) = \pi$. Therefore, $\Lambda_f(n + 1) \subseteq \Lambda_u(n - 1)$. By Lemma 2.5, $\Lambda_f(n + 1) = \Lambda_u(n - 1)$. \square

Corollary 2.8. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. Then $e(\bar{u}) = e = \begin{cases} p - 1 & \text{if } p > 2 \\ 2 & \text{if } p = 2 \end{cases}$. In particular, $\text{Norm}_{\mathbb{F}_p}^{\text{sep}}(\mathcal{A}_{\bar{u}})$ is an extension of a finite group of order dividing e by $\mathcal{A}_{\bar{u}}$.*

3. ABELIAN EXTENSIONS AND TORSION SERIES

Consider the following notation:

$$\begin{aligned} K_n &= \mathbb{Q}_p(\Lambda_f(n)) & K &= \bigcup_{n \geq 1} K_n \\ \mathfrak{G}_n &= \text{Gal}(K_n/\mathbb{Q}_p) & \mathfrak{G} &= \varprojlim \mathfrak{G}_n = \text{Gal}(K/\mathbb{Q}_p) \end{aligned}$$

For the remainder of the note, we will assume that for each n , K_n is generated by any single element of $\Omega_f(n)$, or equivalently, $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$. In this section, we show that \mathfrak{G} is abelian, and that \bar{u} commutes with a torsion series of order e .

Call a sequence $\{\pi_n\}_{n \geq 0}$ of elements in Λ_f *f-consistent* if $\pi_0 = 0$, $\pi_1 \neq 0$, and $f(\pi_{n+1}) = \pi_n$ for all $n \geq 0$ (see [8, Page 329]); in particular, $\pi_n \in \Omega_f(n)$ for all

$n > 0$. By Lemma 2.2, for $n > 0$, K_n/\mathbb{Q}_p is totally ramified of degree $(p-1)p^{n-1}$ and $|G_n| = (p-1)p^{n-1}$.

Fix an f -consistent sequence $\{\pi_n\}_{n \geq 0}$ and let $\mathbf{u}_n \in \mathfrak{G}_n$ be defined by $\mathbf{u}_n(\pi_n) = u(\pi_n)$. Since the coefficients of u are fixed by \mathbf{u}_n , we have $\mathbf{u}_n^i(\pi) = u^{\circ i}(\pi)$ for all i . Clearly, \mathbf{u}_1 is trivial, as is \mathfrak{G}_1 if $p = 2$.

Lemma 3.1. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair, and $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$.*

- (1) *If $p > 2$, then the Sylow p -subgroup of \mathfrak{G}_n is cyclic and generated by \mathbf{u}_n for all $n \geq 1$.*
- (2) *If $p = 2$, then \mathfrak{G}_n contains a cyclic subgroup of order 2^{n-2} generated by \mathbf{u}_n for all $n \geq 3$.*

In both cases, $\mathbf{u}_{n+1}|_{\mathfrak{G}_n} = \mathbf{u}_n$, and so $\mathbf{u} = \varprojlim \mathbf{u}_n$ generates a procyclic subgroup of \mathfrak{G} of index 2.

Proof. The result follows immediately from Proposition 2.7. If $p > 2$, $\mathbf{u}_n^i = 1$ if and only if $p^{n-1} \mid i$. If $p = 2$ and $n \geq 3$, $\mathbf{u}_n^i = 1$ if and only if $2^{n-2} \mid i$. In both cases, $\mathbf{u}_{n+1}(\pi_n) = \mathbf{u}_{n+1}(f(\pi_{n+1})) = f(\mathbf{u}_{n+1}(\pi_{n+1})) = f \circ u(\pi_{n+1}) = u \circ f(\pi_{n+1}) = \mathbf{u}_n(\pi_n)$. \square

Lemma 3.2. *Suppose $\mathbf{g}, \mathbf{h} \in \mathfrak{G}$ and $g, h \in \mathcal{S}_0(\mathbb{Z}_p)$ such that for some $\pi \in K$, $\mathbf{g}(\pi) = g(\pi)$ and $\mathbf{h}(\pi) = h(\pi)$. Then $\mathbf{gh}(\pi) = h \circ g(\pi)$.*

Proof. A direct computation yields the result: $\mathbf{gh}(\pi) = \mathbf{g}(h(\pi)) = h(\mathbf{g}(\pi)) = h \circ g(\pi)$. \square

Lemma 3.3. *Suppose $h_1, h_2 \in \mathbb{Z}_p[[x]]$ and k is an integer such that $h_1(\pi_n) \equiv h_2(\pi_n) \pmod{\pi_n^k}$ for infinitely many n . Then $\bar{h}_1(x) \equiv \bar{h}_2(x) \pmod{x^k}$.*

Proof. Suppose $\bar{h}_1(x) \equiv \bar{h}_2(x) + \bar{d}x^m \pmod{x^{m+1}}$ for some $d \in \mathbb{Z}_p^\times$ and $m > 0$. Pick n large enough so that $v_p(\pi_n^{m+1}) \leq 1$ and $h_1(\pi_n) \equiv h_2(\pi_n) \pmod{\pi_n^k}$. Then $h_1(\pi_n) \equiv h_2(\pi_n) + d\pi_n^{m+1} \pmod{\pi_n^{m+1}}$, which implies $m \geq k$. \square

Remark 3.4. Let $\pi \in \Omega_f(n)$. The Galoisness of $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is equivalent to the following: for each $\pi' \in \Omega_f(n)$ there exists a $g_{\pi'} \in \mathcal{G}_0(\mathbb{Z}_p)$ such that $g_{\pi'}(\pi) = \pi'$. As such, all the Galois automorphisms are “locally analytic.” On the other hand, the relation between \mathbf{u} , \mathbf{u}_n , and u suggests that at least some of the Galois automorphisms are “globally analytic”; in fact, our main result aims to show that they all are. We take a step in that direction by partially extending the relation between \mathbf{u} , \mathbf{u}_n , and u to other elements of the Galois group. For $\mathbf{g} \in \mathfrak{G}$, write $\mathbf{g}(\pi_n) = \sum_{i=1}^{\infty} c_{i,n} \pi_n^i$, where the coefficients $c_{i,n}$ are Teichmüller representatives, and let $g_n(x) = \sum_{i=1}^{\infty} c_{i,n} x^i$. Note that $\mathbf{g}^i(\pi_n) = g_n^{\circ i}(\pi_n)$ for all i . We will call the sequence $\{g_n\}$ the *realization* of \mathbf{g} . Let $\Gamma = \{\sum_{i=1}^{\infty} c_i x^i \in \mathcal{S}_0(\mathbb{Z}_p) \mid c_i^p = c_i\}$. The topology of $\mathbb{Z}_p[[x]]$ induced by the additive \mathbb{Z} -valued valuation v_x is equivalent to the product topology of $\mathbb{Z}_p^{\mathbb{N}}$ when each copy of \mathbb{Z}_p has the discrete topology. Tychonoff’s theorem thus implies that Γ is a compact subset of $\mathbb{Z}_p[[x]]$. So $\{g_n\}$ must have an accumulation point $g \in \Gamma$.

Lemma 3.5. *With the above notation, if $\{g_n\}$ is a realization of $\mathbf{g} \in \mathfrak{G}$ with an accumulation point g , then $\bar{g} \in \text{Norm}_{\mathbb{F}_p}(\bar{u})$.*

Proof. By Lemma 3.2, $\mathbf{u}\mathbf{g}(\pi_n) = g_n \circ u(\pi_n)$ and $\mathbf{g}\mathbf{u}^t(\pi_n) = u^{\circ t} \circ g_n(\pi_n)$ for all n . Let $\{g_{n_\ell}\}$ be a subsequence of $\{g_n\}$ which converges to g . Given $k > 0$, pick l large enough such that if $\ell \geq l$ then $g(x) \equiv g_{n_\ell}(x) \pmod{x^k}$. Thus, if $\ell \geq l$, we have the following congruences mod $\pi_{n_\ell}^k$.

$$\begin{aligned} g \circ u(\pi_n) &\equiv \mathbf{u}\mathbf{g}(\pi_{n_\ell}) \\ &= \mathbf{g}\mathbf{u}^t(\pi_{n_\ell}) \\ &\equiv u^{\circ t} \circ g_n(\pi_{n_\ell}) \end{aligned}$$

Lemma 3.3 implies $\bar{u} \circ \bar{g} \equiv \bar{g} \circ \bar{u}^{\circ t} \pmod{x^k}$. Since k was arbitrary, our result follows. \square

Remark 3.6. Suppose \mathbf{g} and g are as above. Then $\bar{g} = X_{K_1}(\mathbf{g})$ only if the f -consistent sequence $\{\pi_n\}_{n \geq 1}$ is norm-consistent too—that is, if $N_{K_m/K_n}(\pi_m) = \pi_n$ whenever $m \geq n$.

3.1. Proof that \mathfrak{G} is abelian if $p > 2$.

Lemma 3.7. *Suppose $p > 2$, $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair, and $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$. Then for all $n \geq 1$ there exists an automorphism $\mathbf{w}_n \in \mathfrak{G}_n$ of order $p-1$, and $\mathbf{w}_{n+1}|_{\mathfrak{G}_n} = \mathbf{w}_n$.*

Proof. Following Lemma 2.3 and Corollary 2.4, let ζ_{p-1} be a primitive $p-1$ root of unity, and let \mathbf{w}_1 be the generator of \mathfrak{G}_1 given by $\mathbf{w}(\pi_1) \equiv \zeta_{p-1}\pi_1 \pmod{\pi_1^2}$. Proceeding by induction, suppose for some $n \geq 1$ there exists a $\mathbf{w}_n \in \mathfrak{G}_n$ of order $p-1$. Let $\hat{\mathbf{w}}_{n+1} \in \mathfrak{G}_{n+1}$ be any lifting of \mathbf{w}_n , and let $\mathbf{w}_{n+1} = \hat{\mathbf{w}}_{n+1}^{p^n}$. \square

Lemma 3.8. *Suppose $p > 2$. Let $\rho_n = \mathbf{w}_n(\pi_n)$. Then $\{\rho_n\}$ is an f -consistent sequence, and $\rho_n \equiv \zeta_{p-1}\pi_n \pmod{\pi_n^2}$.*

Proof. The f -consistency can be directly verified: $f(\rho_{n+1}) = f(\mathbf{w}_{n+1}(\pi_{n+1})) = \mathbf{w}_{n+1}(f(\pi_{n+1})) = \mathbf{w}_n(\pi_n) = \rho_n$.

Lemma 2.3 provides the second part of the result for $n = 1$, so we proceed by induction on n . Suppose that for some $n \geq 1$, $\rho_n \equiv \zeta_{p-1}\pi_n \pmod{\pi_n^2}$. By Lemma 2.2, $v_p(\pi_n^2) = 2/(p^{n-1}(p-1)) > v_p(\pi_{n+1}^{p+1}) = (p+1)/(p^n(p-1))$, and so $\rho_n \equiv \zeta_{p-1}\pi_n \pmod{\pi_{n+1}^{p+1}}$. By our hypothesis on the commuting pair, $f(x) \equiv ax^p \pmod{(p, x^{p+1})}$ for some $a \in \mathbb{Z}_p^\times$. And by Lemma 2.2, $v_p(\pi_{n+1}^{p+1}) = v_p(\rho_{n+1}^{p+1}) = (p+1)/(p^n(p-1)) < 1 = v_p(p)$. Thus, $\rho_n = f(\rho_{n+1}) \equiv a\rho_{n+1}^p \pmod{\pi_{n+1}^{p+1}}$. Finally, $\zeta_{p-1}\pi_n = \zeta_{p-1}f(\pi_{n+1}) \equiv a\pi_{n+1}^p \pmod{\pi_{n+1}^{p+1}}$. Therefore, $a\rho_{n+1}^p \equiv \zeta_{p-1}a\pi_{n+1}^p \pmod{\pi_{n+1}^{p+1}}$, which implies our result. \square

Proposition 3.9. *Suppose $p > 2$ and $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. If $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$ then $\mathfrak{G} \cong Z_{p-1} \times \mathbb{Z}_p$. In particular, \mathfrak{G} is abelian.*

Proof. Let $\mathbf{w} = \varprojlim \mathbf{w}_n$ and $\mathbf{u} = \varprojlim \mathbf{u}_n$. Then $\langle \mathbf{u} \rangle \cong \mathbb{Z}_p$ is a normal subgroup of \mathfrak{G} since for each n , \mathbf{u}_n generates the unique Sylow p -subgroup of \mathfrak{G}_n by Lemma 3.1. Therefore, $\mathbf{w}\mathbf{u}\mathbf{w}^{-1} = \mathbf{u}^t$ for some $t \in \mathbb{Z}_p$. Moreover, $\mathbf{w}\mathbf{u}\mathbf{w}^{-1} = \mathbf{w}^p\mathbf{u}\mathbf{w}^{-p} = \mathbf{u}^{t^p}$. So t must be a $p-1$ root of unity. We will complete the proof by showing that $t \equiv 1 \pmod{p}$, and hence $t = 1$.

Following the notation and result of Lemma 3.8, write $\rho_2 = \zeta_{p-1}\pi_2 + c_2\pi_2^2 + c_3\pi_2^3 + \cdots$ with $c_i \in \mathbb{Z}_p$. Recall from the hypothesis on the commuting pair that

$u(x) \equiv x + bx^p \pmod{(p, x^{p+1})}$ for some $b \in \mathbb{Z}_p^\times$, and so $u^{\circ t}(x) \equiv x + tbx^p \pmod{(p, x^{p+1})}$. The following congruences are mod π_2^{p+1} .

$$\begin{aligned}
 \rho_2 + b\zeta_{p-1}\pi_2^p &\equiv \rho_2 + b\rho_2^p \\
 &\equiv u(\rho_2) \\
 &= u(\mathfrak{w}(\pi_2)) \\
 &= \mathfrak{w}(u(\pi_2)) \\
 &= \mathfrak{w}u(\pi_2) \\
 &= \mathfrak{u}^t \mathfrak{w}(\pi_2) \\
 &\equiv \mathfrak{u}^t(\zeta_{p-1}\pi_2 + c_2\pi_2^2 + c_3\pi_2^3 + \cdots) \\
 &= \zeta_{p-1}\mathfrak{u}^t(\pi_2) + c_2\mathfrak{u}^t(\pi_2)^2 + c_3\mathfrak{u}^t(\pi_2)^3 + \cdots \\
 &= \zeta_{p-1}u^{\circ t}(\pi_2) + c_2u^{\circ t}(\pi_2)^2 + c_3u^{\circ t}(\pi_2)^3 + \cdots \\
 &\equiv \zeta_{p-1}(\pi_2 + tb\pi_2^p) + c_2\pi_2^2 + c_3\pi_2^3 + \cdots \\
 &= \rho_2 + tb\zeta_{p-1}\pi_2^p.
 \end{aligned}$$

Therefore, $t \equiv 1 \pmod{p}$, concluding the proof. \square

Corollary 3.10. *Suppose $p > 2$. Then $\mathfrak{G}_n \cong Z_{p-1} \times Z_{p^{n-1}}$.*

3.2. Proof that \mathfrak{G} is abelian if $p = 2$.

Proposition 3.11. *Suppose $p = 2$ and $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. If $\mathbb{Q}_2(\pi)/\mathbb{Q}_2$ is Galois for all $\pi \in \Lambda_f$ then $\mathfrak{G} \cong Z_2 \times Z_2$. In particular, \mathfrak{G} is abelian.*

Proof. Write $\bar{f}(x) = \varphi(x^p)$ where $\varphi(x) \in \mathcal{S}_0(\mathbb{F}_p)$. Observe that φ and \bar{u} commute.

If $\varphi \in \mathcal{A}_{\bar{u}}$, then $\varphi = \bar{u}^{\circ t}$ for some $t \in \mathbb{Z}_p$. Therefore, $u^{\circ -t} \circ f$ has the following two properties: it is congruent to $x^p \pmod{p}$, and its linear coefficient is a uniformizer in \mathbb{Z}_p . In other words, $u^{\circ -t} \circ f$ is an endomorphism of a height-one formal \mathbb{Z}_p -module. Since f and u commute with $u^{\circ -t} \circ f$, they must both be endomorphisms of the same formal group. Our result follows.

If $\varphi \notin \mathcal{A}_{\bar{u}}$, then by Theorem 2.1, $\text{Norm}_{\mathbb{F}_p}^{\text{sep}}(\mathcal{A}_{\bar{u}})$ must be abelian. By Lemma 3.5, \mathfrak{G} must be abelian as well.

Let $\Omega_f(2) = \{\beta, \beta'\}$ and $\Omega_f(3) = \{\gamma_1, \gamma_2, \gamma'_1, \gamma'_2\}$ such that $f(\gamma_1) = f(\gamma_2) = \beta$ and $f(\gamma'_1) = f(\gamma'_2) = \beta'$. From Proposition 2.7, we know that $\mathfrak{u}_2(\beta) = u(\beta) = \beta'$, and so $\mathfrak{u}_3(\gamma_1)$ is a root of $f(x) - \beta'$; say $\mathfrak{u}_3(\gamma_1) = u(\gamma_1) = \gamma'_1$. Since $\gamma_1 \in \Lambda_u(1)$, $\mathfrak{u}_3^2(\gamma_1) = u^{\circ 2}(\gamma_1) = \gamma_1$. Clearly, $\mathfrak{u}_3(\gamma_2) = \gamma'_2$. Let $\mathfrak{w}_3 \in \mathfrak{G}_3$ be given by $\mathfrak{w}_3(\gamma_1) = \gamma'_2$. Then $\mathfrak{w}_3^2(\gamma_1) = \mathfrak{w}_3(\gamma'_2) = \gamma_1$ since $\mathfrak{u}_3(\gamma'_2) = \gamma_2$. Thus, \mathfrak{G}_3 contains two elements of order 2, and so it is not cyclic. \square

Corollary 3.12. *Suppose $p = 2$. Then for $n \geq 2$, $\mathfrak{G}_n \cong Z_2 \times Z_{2^{n-2}}$.*

Corollary 3.13. *The group $\text{Norm}_{\mathbb{F}_p}^{\text{sep}}(\mathcal{A}_{\bar{u}})$ is abelian.*

The f -consistent sequence defined in Lemma 3.8 for $p > 2$ has an analogue for $p = 2$: let $\mathfrak{w} \in \mathfrak{G} \cong Z_2 \times Z_{2^{n-2}}$ be the generator of Z_2 , and define $\rho_n = \mathfrak{w}(\pi_n)$. For each n , write the π_n -adic expansion of ρ_n as $\rho_n = \mathfrak{w}(\pi_n) = \sum_{i=1}^{\infty} c_{i,n} \pi_n^i$, where $c_{1,n}$ is a fixed primitive $p-1$ root of unity ζ_{p-1} , and $c_{i,n}^p = c_{i,n}$. Let $w_n(x) = \sum_{i=1}^{\infty} c_{i,n} x^i$. Recall from Remark 3.4 that $\{w_n\}$ is a realization of \mathfrak{w} in the compact set Γ , and so it has a convergent subsequence $\{w_{n_\ell}\}$ and a corresponding accumulation point w .

Lemma 3.14. *Suppose $p = 2$. Then $w_n \equiv x + x^2 \pmod{x^3}$ for all n , and so $w(x) \equiv x + x^2 \pmod{x^3}$ as well.*

Proof. This follows from the fact that $K_2 \not\subset K^{\mathfrak{w}}$; see for instance [13, Chapter IV]. \square

3.3. Torsion series over \mathbb{F}_p . We end this section with the construction of a torsion power series over \mathbb{F}_p of order e that commutes with \bar{f} and \bar{u} .

Proposition 3.15. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. Then \bar{w} commutes with \bar{u} . Moreover, \bar{w} is torsion of order $e = e(\bar{u})$.*

Proof. For $k > 0$, pick l such that if $\ell > l$ then $v_p(\pi_{n_\ell}^{k+1}) \leq 1$ and $v_x(w - w_{n_\ell}) \geq k+1$.

By Lemma 3.2, $\mathfrak{w}u(\pi_n) = u \circ w_n(\pi_n)$ and $\mathfrak{u}w(\pi_n) = w_n \circ u(\pi_n)$ for all n . Recalling that G is abelian, we have the following congruences mod $\pi_{n_\ell}^{k+1}$ for $\ell > l$.

$$\begin{aligned} u \circ w(\pi_{n_\ell}) &\equiv u \circ w_n(\pi_{n_\ell}) \\ &= \mathfrak{w}u(\pi_{n_\ell}) \\ &= \mathfrak{u}w(\pi_{n_\ell}) \\ &= w_n \circ u(\pi_{n_\ell}) \\ &\equiv w \circ u(\pi_{n_\ell}) \end{aligned}$$

By Lemma 3.3, $\bar{u} \circ \bar{w} \equiv \bar{w} \circ \bar{u} \pmod{x^{k+1}}$. Since k was arbitrary, it follows that $\bar{u} \circ \bar{w} = \bar{w} \circ \bar{u}$.

If $\ell > l$, then $\pi_{n_\ell} = \mathfrak{w}^e(\pi_{n_\ell}) = w_n^{\circ e}(\pi_{n_\ell}) \equiv w^{\circ e}(\pi_{n_\ell}) \pmod{\pi_{n_\ell}^{k+1}}$. By Lemma 3.3, $\bar{w}^{\circ e}(x) \equiv x \pmod{x^{k+1}}$. Since k was arbitrary, we see that the order of \bar{w} divides e . If $p > 2$, then the order is exactly $p - 1$ because $w'(0)$ is a primitive $p - 1$ root of unity. If $p = 2$, then the order of \bar{w} is 2 by Lemma 3.14. \square

Corollary 3.16. *Suppose $\theta \in \mathcal{S}_0(\mathbb{F}_p)$ is a torsion series of order e that commutes with \bar{u} . If $\theta'(0) = \bar{w}'(0)$ then $\theta = \bar{w}$.*

Therefore, \bar{w} is independent of the choice of $\{w_n\}$.

By [8, Corollary 6.2.1], the noninvertible half of a commuting pair must be of the form $\bar{f}(x) = \varphi(x^{p^d})$ for some $d > 0$ and $\varphi \in \kappa[[x]]$ invertible; d is called the *radicial degree* of f . Since our commuting pair is minimal, then $d = 1$.

Corollary 3.17. *The power series \bar{w} and φ commute.*

If $p = 2$, then $\bar{w} \in \text{Nott}(\mathbb{F}_2)$. Torsion elements of the Nottingham group are well understood and well behaved. For instance, all torsion elements of $\text{Nott}(\mathbb{F}_p)$ have order p^d for some d . Moreover, since any pro- p group can be embedded in $\text{Nott}(\mathbb{F}_p)$, then in fact there exists a torsion element of order p^d for every d . Two torsion elements of order p , $x + ax^\ell + \dots$ and $x + bx^m + \dots$, are conjugate over $\text{Nott}(\mathbb{F}_p)$ if and only if $a = b$ and $\ell = m$. The situation is slightly less tidy for $d > 1$. In fact, for some time, “an element of order p^2 [was] still not known” ([1, page]). In [9], the results of [4] are generalized via local-class-field-theoretic methods that associate to torsion elements of $\text{Nott}(\mathbb{F}_p)$ certain characters on $1 + x\mathbb{F}_p[[x]]$, and explicit elements of any order are exhibited.

Corollary 3.18. *Suppose $p = 2$. Then $w(x)$ is conjugate over $\mathcal{G}_0(\mathbb{F}_p)$ to $\sum_{i=1}^{\infty} x^i$.*

Proof. This follows directly from [4, Theorem]. \square

4. PROOF OF MAIN RESULT

Recall from Remark 1.3 that if ζ_e is a primitive e^{th} root of unity, then $z(x) = \sum_{i=1}^{\infty} d_i x^i = [\zeta_e]_f(x) = L_f^{\circ -1}(\zeta_e L_f(x)) \in \mathcal{G}_0(\mathbb{Q}_p)$ is the unique e -torsion series with linear coefficient $d_1 = \zeta_e$ that commutes with f and u . Let $z_k(x) = \sum_{i=1}^k d_i x^i$ and continue to write $f(x) = \sum_{i=1}^{\infty} a_i x^i$. Clearly, $z_1(x) = \zeta_e x \in \mathcal{G}_0(\mathbb{Z}_p)$ and $z_1 \circ f \equiv f \circ z_1 \pmod{x^2}$. Moreover, if $p = 2$ and $z_2(x) = -x + d_2 x^2$, then $f \circ z_2 \equiv z_2 \circ f \pmod{x^3}$ implies $d_2 = 2a_2/(a_1^2 - a_1) \in \mathbb{Z}_2^{\times}$.

The proof of our main result, that $z \in \mathcal{G}_0(\mathbb{Z}_p)$, will proceed inductively. Let $\delta = 1$ if $p > 2$ and $\delta = 2$ if $p = 2$. Suppose for some $k \geq \delta$ that $z_k \in \mathcal{G}_0(\mathbb{Z}_p)$ and $z_k \circ f \equiv f \circ z_k \pmod{x^{k+1}}$. For $z_{k+1}(x) = z_k(x) + d_{k+1}x^{k+1}$ to commute with $f(x) \pmod{x^{k+2}}$, we must have

$$d_{k+1}(a_1^{k+1} - a_1)x^{k+1} \equiv f \circ z_k(x) - z_k \circ f(x) \pmod{x^{k+2}}$$

Therefore, our proof will be completed once we show that $\bar{f} \circ \bar{z}_k(x) - \bar{z}_k \circ \bar{f}(x) \equiv 0 \pmod{x^{k+2}}$ in Proposition 4.4 below.

Recall that $\{\pi_n\}$ is a fixed f -consistent sequence, $\mathfrak{w} \in \mathfrak{G}$ is an automorphism of order e , and $\rho_n = \mathfrak{w}(\pi_n)$ is f -consistent as well. The proof of the main result will rely on the relationship between the valuation of $\rho_n - g(\pi_n)$ for some $g \in \mathcal{G}_0(\mathbb{Z}_p)$ and the extent to which the series g commutes with f . We explore that relation in more detail in the next three lemmas.

Lemma 4.1. *Suppose for some $n > 0$, $\rho_n \equiv g(\pi_n) + c_{m,n}\pi_n^m \pmod{\pi_n^{m+1}}$, where $g \in \mathbb{Z}_p[[x]]$ and $c_{m,n} \in \mathbb{Z}_p^{\times}$. Suppose further than $f \circ g \equiv g \circ f \pmod{x^{k+1}}$. If $m \neq p^{n-1}$ then $mp \geq \min\{v_{K_n}(\rho_{n-1} - g(\pi_{n-1})), k+1\}$. The inequality is strict if $v_{K_n}(a_p \pi_n^{mp}) > v_{K_n}(a_1 \pi_n^m)$.*

Proof. Write $\rho_n = g(\pi_n) + c_{m,n}\pi_n^m + D\pi_n^{m+1}$ for some $D \in \mathbb{Z}_p[[\pi_n]]$. Then

$$\begin{aligned} f(\rho_n) &= \sum_{i=1}^{\infty} a_i (g(\pi_n) + c_{m,n}\pi_n^m + d\pi_n^{m+1})^i \\ &= f(g(\pi_n)) + a_1 c_{m,n} \pi_n^m + a_p (c_{m,n} \pi_n^m)^p + D_1 p \pi_n^{m+1} + D_2 (\pi_n^{m+1})^p \end{aligned}$$

where $D_1, D_2 \in \mathbb{Z}_p[[\pi_n]]$. If $m \neq p^{n-1}$ then $p^{n-1}(p-1) + m = v_{K_n}(a_1 c_{m,n} \pi_n^m) \neq v_{K_n}(a_p (c_{m,n} \pi_n^m)^p) = mp$, and so by the isosceles triangle principle $v_{K_n}(f(\rho_n) - f(g(\pi_n))) = v_{K_n}(a_1 c_{m,n} \pi_n^m + a_p (c_{m,n} \pi_n^m)^p)$. But $f(\rho_n) - f(g(\pi_n)) = \rho_{n-1} - g(\pi_{n-1}) + M\pi_n^{k+1}$ for some $M \in \mathbb{Z}_p[[\pi_n]]$. Therefore,

$$\begin{aligned} mp &\geq \min\{p^{n-1}(p-1) + m, mp\} \\ &= v_{K_n}(a_1 c_{m,n} \pi_n^m + a_p (c_{m,n} \pi_n^m)^p) \\ &= v_{K_n}(f(\rho_n) - f(g(\pi_n))) \\ &= v_{K_n}(\rho_{n-1} - g(\pi_{n-1}) + M\pi_n^{k+1}) \\ &\geq \min\{v_{K_n}(\rho_{n-1} - g(\pi_{n-1})), k+1\} \end{aligned}$$

□

Lemma 4.2. *Suppose $g \in \mathcal{G}_0(\mathbb{Z}_p)$ and $n \geq \delta$. For each $c \in \mathbb{Z}_p^{\times}$ there exists a unique integer $1 \leq j \leq p-1$ depending on $\bar{c}, \overline{g'(0)}$, and n such that $g \circ u^{\circ j p^{n-\delta}}(\pi_{n+1}) - g(\pi_{n+1}) \equiv c \pi_{n+1}^{p^n} \pmod{\pi_{n+1}^{p^n+1}}$.*

Proof. By Proposition 2.7, $\text{ord}_x(u^{\circ p^{n-\delta}}(x)) = p^n$. Write $u^{\circ p^{n-\delta}}(x) - x = \sum_{i=1}^{\infty} b_i x^i$. Thus, $b_{p^n} \in \mathbb{Z}_p^\times$, and if $1 \leq i < p^n$ then $v_{K_{n+1}}(b_i \pi_{n+1}^i) \geq p^n(p-1) + i > p^n$. So $u^{\circ p^{n-\delta}}(\pi_{n+1}) \equiv \pi_{n+1} + b_{p^n} \pi_{n+1}^{p^n} \pmod{\pi_{n+1}^{p^n+1}}$. A direct computation then shows $u^{\circ j p^{n-\delta}}(\pi_{n+1}) \equiv \pi_{n+1} + j b_{p^n} \pi_{n+1}^{p^n} \pmod{\pi_{n+1}^{p^n+1}}$. So the proof is complete by solving for j in $j g'(0) b_{p^n} \equiv c \pmod{p}$. \square

Lemma 4.3. *Suppose $h \in \mathcal{G}_0(\mathbb{Z}_p)$ such that $h'(0) = \zeta_{p-1}$ if $p > 2$ and $\bar{h}(x) \equiv x + x^2 \pmod{x^3}$ if $p = 2$. If $f \circ h(x) - h \circ f(x) \equiv 0 \pmod{x^{k+1}}$, then there exists $\ell \in \mathbb{Z}_p$ such that $v_{K_n}(\rho_n - h \circ u^{\circ \ell}(\pi_n)) \geq (k+1)/p$ for all n . The inequality is strict if $v_{K_n}(a_p \pi_n^{mp}) > v_{K_n}(a_1 \pi_n^m)$. Moreover, $v_{K_n}(\rho_n - h \circ u^{\circ \ell}(\pi_n)) \neq p^{n-1}$.*

Proof. We will construct a Cauchy sequence of integers $\{\ell_n\}$ for which $v_{K_s}(\rho_s - h \circ u^{\circ \ell_n}(\pi_s)) \geq (k+1)/p$ whenever $s \leq n$.

Let $\ell_1 = 0$. If $\rho_1 = h(\pi_1)$ the result follows trivially. If not, write $\rho_1 \equiv h(\pi_1) + c_{m,1} \pi_1^m \pmod{\pi_1^{m+1}}$ for some $c_{m,1} \in \mathbb{Z}_p^\times$. Note that $m > 1 = p^0$ by Lemma 2.3 and so $p-1+m < mp$. Therefore, by Lemma 4.1, $mp > \min\{v_{K_1}(0), k+1\} = k+1$.

If $p = 2$, let $\ell_2 = 0$ as well. The result follows trivially if $\rho_2 = h(\pi_2)$. Otherwise, write $\rho_2 \equiv h(\pi_2) + c_{m,2} \pi_2^m \pmod{\pi_2^{m+1}}$ for some $c_{m,2} \in \mathbb{Z}_2^\times$. Note that $m > 2$ by Lemma 3.14, and so $2(2-1)+m < 2m$. Therefore, by Lemma 4.1, $2m > \min\{v_{K_2}(\rho_1 - h(\pi_1)), k+1\} = k+1$.

Suppose that for some $n \geq \delta + 1$ there exists an integer ℓ_n for which $v_{K_s}(\rho_s - h \circ u^{\circ \ell_n}(\pi_s)) \geq (k+1)/p$ whenever $s \leq n$.

If $\rho_{n+1} - h \circ u^{\circ \ell_n}(\pi_{n+1}) \equiv c \pi_{n+1}^{p^n} \pmod{\pi_{n+1}^{p^n+1}}$ for some $c \in \mathbb{Z}_p^\times$, then by Lemma 4.2 there exists a $1 \leq j_{n+1} \leq p-1$ such that $h \circ u^{\circ \ell_n} \circ u^{\circ j_{n+1} p^{n-\delta}}(\pi_{n+1}) - h \circ u^{\circ \ell_n}(\pi_{n+1}) \equiv c \pi_{n+1}^{p^n} \pmod{\pi_{n+1}^{p^n+1}}$. If on the other hand $v_{K_{n+1}}(\rho_{n+1} - h \circ u^{\circ \ell_n}(\pi_{n+1})) \neq p^n$, let $j_{n+1} = 0$. Let $\ell_{n+1} = \ell_n + j_{n+1} p^{n-\delta}$. If $\rho_{n+1} = h \circ u^{\circ \ell_{n+1}}(\pi_{n+1})$ then the result follows trivially. Otherwise, write $\rho_{n+1} - h \circ u^{\circ \ell_{n+1}}(\pi_{n+1}) \equiv c_{m,n+1} \pi_{n+1}^m \pmod{\pi_{n+1}^{m+1}}$ for some $c_{m,n+1} \in \mathbb{Z}_p^\times$. Observe that if $s < n+1$, then $u^{\circ p^{n-\delta}}(\pi_s) = \pi_s$ by Proposition 2.7, so that $u^{\circ \ell_{n+1}}(\pi_s) = u^{\circ \ell_n}(\pi_s)$. The choice of j_{n+1} guarantees that $m \neq p^n$. Therefore, by Lemma 4.1, $mp > \min\{v_{K_{n+1}}(\rho_n - h \circ u^{\circ \ell_{n+1}}(\pi_n)), k+1\} = \min\{v_{K_{n+1}}(\rho_n - h \circ u^{\circ \ell_n}(\pi_n)), k+1\} = k+1$. \square

Proposition 4.4. *Suppose $z_k \in \mathcal{G}_0(\mathbb{Z}_p)$ with $z'_k(0) = \zeta_e$ for some $k \geq \delta$. If $p = 2$, suppose that $\bar{z}_2(x) = x + x^2$. If $f \circ z_k(x) - z_k \circ f(x) \equiv 0 \pmod{x^{k+1}}$ then $\bar{f} \circ \bar{z}_k(x) - \bar{z}_k \circ \bar{f}(x) \equiv 0 \pmod{x^{k+2}}$.*

Proof. Write $f \circ z_k(x) - z_k \circ f(x) \equiv dx^{k+1} \pmod{x^{k+2}}$ for some $d \in \mathbb{Z}_p$.

If $p \nmid k+1$ then $d \in p\mathbb{Z}_p$ by [8, Corollary 6.2.1].

If $p \mid k+1$, let $m = (k+1)/p$. For each n , Lemma 4.3 allows us to write $\rho_n \equiv z_k \circ u^{\circ \ell}(\pi_n) + c_n \pi_n^m \pmod{\pi_n^{m+1}}$ for some $\ell \in \mathbb{Z}_p$, where $c_n \in \mathbb{Z}_p$ is a Teichmüller representative. Moreover, the choice of ℓ guarantees that if $m = p^{n-1}$, then $c_n = 0$.

Let N be the least positive integer that satisfies $v_{K_N}(a_1 \pi_N^m) > v_{K_N}(a_p \pi_N^{mp})$; note that $N \geq 2$. By Lemma 4.3 again, $c_{N-1} = 0$. Moreover, for all $n \geq N$, we have $\pmod{\pi_n^{mp+1}}$

$$\begin{aligned} \rho_{n-1} &\equiv z_k \circ u^{\circ \ell}(\pi_{n-1}) + c_{n-1} \pi_{n-1}^m & \rho_{n-1} &= f(\rho_n) \\ &\equiv z_k \circ u^{\circ \ell}(f(\pi_n)) + c_{n-1} f(\pi_n)^m & &\equiv f(z_k \circ u^{\circ \ell}(\pi_n) + c_n \pi_n^m) \\ &\equiv z_k \circ u^{\circ \ell}(f(\pi_n)) + c_{n-1} (a_p \pi_n^p)^m & &\equiv f(z_k \circ u^{\circ \ell}(\pi_n)) + a_p (c_n \pi_n^m)^p \end{aligned}$$

Therefore, $f(z_k \circ u^{\circ\ell}(\pi_n)) + a_p(c_n \pi_n^m)^p \equiv z_k \circ u^{\circ\ell}(f(\pi_n)) + c_{n-1}(a_p \pi_n^p)^m \pmod{\pi_n^{pm+1}}$, and so

$$c_n \equiv \frac{z_k \circ u^{\circ\ell}(f(\pi_n)) - f(z_k \circ u^{\circ\ell}(\pi_n))}{a_p} + c_{n-1}a_p^{m-1} \pmod{\pi_n}$$

Iterating this last congruence, we get

$$c_n \equiv \frac{z_k \circ u^{\circ\ell}(f(\pi_n)) - f(z_k \circ u^{\circ\ell}(\pi_n))}{a_p} \sum_{i=N}^n a_p^{(m-1)(n-i)} \pmod{\pi_n}$$

But $\sum_{i=N}^n a_p^{(m-1)(n-i)} \equiv 0 \pmod{p}$ for infinitely many n , and so too $c_n \equiv 0 \pmod{p}$ for infinitely many n . Thus by Lemma 3.3, $\bar{w} \equiv \bar{z}_k \circ \bar{u}^{\circ\ell} \pmod{x^{m+1}}$.

Now recall that \bar{w} commutes with φ by Corollary 3.17. So $0 = \varphi \circ \bar{w}(x) - \bar{w} \circ \varphi(x) \equiv \varphi \circ \bar{z}_k \circ \bar{u}^{\circ\ell}(x) - \bar{z}_k \circ \bar{u}^{\circ\ell} \circ \varphi(x) \pmod{x^{m+1}}$. And since \bar{u} commutes with \bar{w} by Proposition 3.15, we also have $\varphi \circ \bar{z}_k(x) - \bar{z}_k \circ \varphi(x) \pmod{x^{m+1}}$. Therefore

$$0 \equiv \varphi \circ \bar{z}_k(x^p) - \bar{z}_k \circ \varphi(x^p) \pmod{x^{mp+1}},$$

yielding our desired result since $mp = k + 1$ and $\varphi(x^p) = \bar{f}(x)$. \square

REFERENCES

- [1] R. Camina, ‘Subgroups of the Nottingham group’, *J. Algebra* 196 (1997), no. 1, 101–113.
- [2] J.-M. Fontaine and J.-P. Wintenberger, ‘Le “corps des normes” de certaines extensions algébriques de corps locaux’, *C. R. Acad. Sci. Paris* 288 (1979), 367–370.
- [3] J.-M. Fontaine and J.-P. Wintenberger, ‘Extensions algébriques et corps des normes des extensions APF des corps locaux’, *C. R. Acad. Sci. Paris* 288 (1979) 441–444.
- [4] B. Klopsch, ‘Automorphisms of the Nottingham group’, *J. Algebra* 223 (2000), no. 1, 37–56.
- [5] N. Koblitz, ‘ p -adic numbers, p -adic analysis, and zeta-functions’ Springer, New York, 1977.
- [6] F. Laubie, A. Movahhedi and A. Salinier, ‘Systèmes dynamiques non archimédiens et corps des normes’, *Compos. Math.* 132 (2002) 57–98.
- [7] J. Lubin, ‘One-parameter formal Lie groups over \mathfrak{P} -adic integer rings’, *Ann. Math.* 80 (1964), 464–484.
- [8] J. Lubin, ‘Nonarchimedean dynamical systems’, *Compos. Math.* 94 (1994), 321–346.
- [9] J. Lubin ‘Torsion in the Nottingham group’, *Bull. Lond. Math. Soc.* To appear.
- [10] J. Lubin and J. Tate, ‘Formal complex multiplication in local fields’, *Ann. Math.* 81 (1965), no. 2, 380–387.
- [11] G. Sarkis, ‘Height one commuting dynamical systems over \mathbb{Z}_p ’, *Bull. Lond. Math. Soc.* 42 (2010), no. 3, 381–387.
- [12] S. Sen, ‘On automorphisms of local fields’, *Ann. of Math. (2)* 90 (1969), 33–46.
- [13] J.-P. Serre, ‘Local Fields’ Springer, New York, 1979.

POMONA COLLEGE, 610 N. COLLEGE AVE., CLAREMONT, CA 91711

E-mail address: ghassan.sarkis@pomona.edu

WESLEYAN UNIVERSITY, 265 CHURCH ST., MIDDLETOWN, CT 06459-0128

E-mail address: jspecter@wesleyan.edu